利用 PRTG 构建免费网络监控环境

摘　要：在互联浪潮的推动下，人们的工作和生活已经完全网络化，无论从家庭生活还是单位的日常工作，都需要稳定的网络环境来支撑，尤其是单位，各种业务对基础网络设备的稳定性、可靠性有着更高的要求。对于一般单位的网络管理员来说，不仅需要建设一个具备可靠设备、精心规划的网络，同时还要有监控网络的能力，以便在故障前或实际发生时了解故障情况。PRTG 是一款功能强大的网络设备监控软件，通过它，网络管理员能够知晓内部网络中路由器、防火墙、交换机、服务器、计算机等多种设备的实时状况，并且以图形、图标的形式展现出来，方便阅读了解。能实时了解设备运行情况和收到提前预警对于事务繁杂的中小型单位的网络管理员来说是非常重要的。

关键词：网络设备监控；PRTG；用户界面；监控数据
中图分类号：TN948.3　　文献标识码：A
文章编号：1671-0134（2019）05-109-04　　DOI：10.19483/j.cnki.11-4653/n.2019.05.036

文 / 张智伟

随着互联网的不断扩张繁衍，人们的工作、生活已经无法离开网络。网络覆盖越广，需要维护的网络基础设备也越来越多，尤其是单位，传统的以人工巡查为主的方法和管理手段已经不能适应新的形势，集中监控、主动收集设备运行参数、运用历史数据曲线分析，及早发现故障隐患，实现规范化、科学化设备运行维护已经是网络自动运维的趋势。网络设备虽然不会经常出现故障，但是它的安全运行却是最让人牵肠挂肚的，尤其是防火墙、路由器、核心交换机等重要的基础网络设施，一旦停摆，工作几乎停滞，后果不堪设想。使用网络监控工具可以实时查看各种网络设备和应用程序的实时和历史数据，提前发现问题，使网络安全管理工作事半功倍。

1. 了解 PRTG

1.1 PRTG 简介

PRTG 全称为 Paessler Router Traffic Grapher，是一个功能强大的网络监控应用程序，基于 Windows 系统，适用于大中小型网络，并且能够进行流量、数据包、应用程序、带宽、云服务、数据库、虚拟环境、正常运行时间、端口、IP，硬件、安全性、Web 服务、磁盘使用、物理环境，物联网设备等可以想象的几乎所有内容。为网络管理员提供实时读数和周期性使用趋势，以优化路由器、防火墙、服务器等各种网络组件的效率、布局和设置。

该软件使用简单网络管理协议（SNMP）、Windows Management Instrumentation（WMI）、数据包嗅探器、NetFlow（以及 IPFIX，sFlow 和 jFlow）以及许多其他行业设置和使用的监控网络标准协议，全天候运行，不断记录网络使用参数和网络系统的可用性，记录的数据存储在内部数据库中以供分析。

PRTG 提供两种监视网络的选项：本地 PRTG 和 Paessler 公司的云托管 PRTG。在使用本地 PRTG 时，核心服务器和本地探针将在本地网络中运行；云托管 PRTG 由云端运行核心服务器和托管探针。本地 PRTG 和云托管 PRTG 上使用的监控配置和查看监控数据的 PRTG Web 界面都是相同的。

如果想在本地使用 PRTG，只需从官方网站下载并安装在 Windows 计算机上即可；如果想使用云托管 PRTG，只需到 https://my-prtg.com 上自行创建账号使用，不需要下载任何程序。

1.2 PRTG 架构

PRTG 组件分为三大类：系统部件、用户界面和系统管理程序。

（1）系统部件分为：核心服务器和探针。核心服务器是 PRTG 的核心部分，包括数据存储、Web 服务器、报告引擎、通知系统等。核心服务器配置为长期运行的 Windows 服务；探针是 PRTG 真正执行监控的部分。PRTG 内部有本地探针、远程针和集群探针，云托管 PRTG 中有托管探针和远程探针，所有监控数据都收集到中央核心服务器。探针配置为长期运行的 Windows 服务。

核心服务器执行如下进程：监视对象的配置管理（例如服务器、工作站、打印机、交换机、路由器、

虚拟机等）/ 管理和配置连接的探针 / 集群管理 / 监测结果的数据库 / 通知管理包括用于电子邮件传递的邮件服务器 / 报告生成器和调度程序 / 用户账户管理 / 数据清除（例如删除超过 365 天的数据）/Web 服务器和 API 服务器。

探针通过 PRTG 在设备（例如计算机、路由器、服务器或防火墙）上创建的传感器执行实际监控并在核心服务器接收其配置，运行监控进程，将监控数据收集到核心服务器。

（2）用户界面分为 Web 界面、 Desktop 界面和手机 APP。基于 Ajax 的 Web 界面用于配置设备和传感器、查看监控结果以及配置系统管理和用户管理。Desktop 界面是一种跨平台 PC 端应用程序，下载安装到本地计算机，连接到不同的 PRTG 核心服务器查看其数据；用于移动网络监控的 PRTG APP，可适配 IOS 和 Android 手机，随时随地可以监控网络状况。

（3）系统管理程序分为核心服务器系统上的 PRTG 管理工具和远程探针系统上的 PRTG 管理工具。前者用于在内部配置 PRTG 中的基本核心服务器设置，例如管理员登录、Web 服务器 IP 和端口、探针连接设置、群集模式、系统语言等；后者用来配置基本探针设置，例如探针名称、IP 和服务器连接设置等。

2. 部署 PRTG

推荐将 PRTG 的核心服务器（Core Server）和远程探针（Remote Probes）安装并运行在 X64 架构的 PC 或者服务器上，硬件最低配置：双核 CPU/3GB 内存 / 硬盘空间 250 GB，首选 64 位 Microsoft Windows 7/Microsoft Windows Server 2008 R2 以上操作系统，确保已安装 .NET Framework 4.7.2 版本。注意：不支持 Windows Server 2012 的 Core 模式以及 Minimal Server 操作界面。

2.1 开启核心服务器 SNMP 功能

PRTG 需要使用 SNMP 来读取核心服务器数据，SNMP 在 Windows 系统中默认是关闭的，需要手动打开。例如设置 Windows 2008 Server R2，打开控制面板 – 点击程序 – 点击打开或关闭 Windows 功能，弹出服务器管理器，找到功能摘要，点击添加功能，勾选 SNMP 服务，包括 SNMP 服务和 SNMP WMI 提供程序，然后点击确定。

2.1.1 配置 SNMP 选项

打开控制面板，点击管理工具 – 服务，双击 SNMP SERVICE，在安全选项中添加团体名称（需与被监控设备设置一致），选择只读或读写都可以，在接受来自以下主机的 SNMP 数据包选项中添加想要监控的设备的 IP 地址，点击确定。

2.1.2 开启防火墙 161 端口

打开控制面板，点击 Windows 防火墙 – 高级设置，在入站规则中查找 SNMP 服务（UDP In），没有可自建，选择 UDP，端口 161，高级配置勾选域、公用、专用，点击确定生效。

2.2 开启被监控设备 SNMP

被监控设备需要开启 SNMP 并设置必要的参数，PRTG 才能够实现监视流量自动绘制流量图的功能。以 H3C 交换机为例，其他品牌交换机可自行参考相关命令。

<H3C>system–view

[H3C]snmp–agent

[H3C]snmp–agent local–engineid xxxxxxxxxxxxxxxx（设备引擎 ID）

[H3C]snmp–agent community read xxxxxx（团体名称，需与核心服务器设置一致）

[H3C]snmp–agent sys–info version v1 v2c

[H3C]snmp–agent target–host trap address udp–domain xxxx.xxx.xxx.xxx（PRTG 服务器地址） params securityname 1 v2c

2.3 安装 PRTG

完成上述工作后，从 PRTG 官网下载自带许可的 30 天试用版 PRTG，点击安装，一直默认下一步，直至完成。核心服务器桌面上会自动创建 PRTG Network Monitor 图标，登录用户名和密码均为 prtgadmin。首次登录，PRTG 会自动创建第一个探针，PRTG 的本地探针与 PRTG 核心服务器在同一台计算机上运行，用户可以选择自动扫描设备或手动添加扫描设备提供设备 IP 地址等信息。完成设备添加后，在设备名称上点击右键，出现文本菜单，运行自动发现，PRTG 可以检查、创建传感器，如果找到可以使用且尚未创建的有用传感器，将会创建推荐传感器列表，供用户选择，以确保不会错过设备重要的监控信息。当然，对于熟悉设备情况的网络管理员来说，也可以选择手动添加传感器。

3. PRTG 功能实现

3.1 监控数据采集

PRTG 依托 10,000 多种自带的传感器，采用 Ping、SNMP、WMI、性能计数器、HTTP、SSH、数据包嗅探、NetFlow、sFlow、jFlow、PowerShell、推送消息接收程序、PRTG Cloud 等技术，涵盖监控目标如 Windows、Linux/

MacOS、虚拟化操作系统、存储和文件服务器、电子邮件服务器、数据库、云服等类型，可实现设备的可用性 / 正常运行时间、带宽 / 流量、网络速度 / 性能、CPU 使用情况、磁盘使用情况、内存使用情况、硬件参数、网络基础设施的监控。

常用的网络监控传感器有：

Ping 传感器：将运行探针的计算机上的 ICMP 回送请求 Ping 发送到被监控设备，以监视设备的可用性。默认值为每个扫描间隔 5 个 Ping，可以显示以下内容：Ping 时间 / 每个间隔使用多个 Ping 时的最小 Ping 时间 / 每个间隔使用多个 Ping 时的最大 Ping 时间 / 每个间隔使用多个 Ping 时数据包丢失百分比。

HTTP 传感器：使用超文本传输协议（HTTP）监视 Web 服务器，可以显示了网页的加载时间，是监控网站是否可访问的最简单方法。

HTTP Advanced 传感器：使用超文本传输协议（HTTP）监视网页的源代码，支持身份验证，内容检查和其他高级参数。可以显示加载时间 / 收到的字节数 / 下载带宽（速度）/ 第一个字节的时间。

SNMP 传感器：PRTG 中种类最多的传感器，充分利用 SNMP 的简单网络管理的特性，将收集到的流量信息、性能、负载、磁盘空间等设备参数，以图形或表格方式展示出来。Cisco、DELL、HP、联想等公司专门的提供了各种定制 SNMP 传感器应用于自身设备的监控。

其中，SNMP 流量传感器是监控网络基础设备最主要的传感器，常用于路由器、防火墙、交换机等网络基础设施监控，添加该传感器时，需要提供被监控设备的 IP 地址、团体名称（必须与网络设备设置的一致）。设备的每个端口都有一个流量传感器，可以显示以下内容：流量流入 / 流出 / 流量总数 / 错误进出 / 丢弃进出 / 单播数据包进出 / 非单播数据包进出 / 组播数据包进出 / 广播包进出 / 未知的协议，传感器实际显示通道取决于被监控设备和传感器的设置。

3.2 传感器状态提示

在 PRTG 设备树中，通常会为每个设备创建多个传感器，可以监控设备的不同方面，使用简单的颜色代码，可以醒目的显示网络中正在发生的事情。

传感器的颜色始终显示其当前状态，同时，传感器状态显示亦有层次结构，无论何时显示传感器状态（在设备树或地理地图上），在层次结构中越高，其在显示传感器状态时的优先级越高。例如，设备的所有传感器都处于正常状态，若其中一个传感器达到停机状态，则此设备的整体状态将显示停机（例如在树形图视图中以红色显示），因为停机状态在层次结构中最高。

表 1　传感器显示状态列表（层次由高到低）

图标	颜色	状态名称	含义
!!	红色	停机	1.PRTG 无法访问设备，或传感器已更改为错误状态，传感器在显示此状态时不会在其通道中记录任何数据。2. 可能是传感器通道设置中设置的错误限制，或者由于传感器查找而导致的错误状态，在这种情况下，尽管传感器显示错误，但是还会继续记录所有传感器通道中的数据
!!	绿 / 红	停机（部分）	在集群中，至少一个节点将此传感器报告为关闭，而至少一个其他节点将同一传感器报告为关闭
!	亮红	停机（已确认）	传感器为停机，PRTG 用户已通过“确认报警”功能确认该状态。对于已确认的警报，不会发送进一步的通知。要设置此传感器状态，请右键单击处于关闭状态的传感器，然后从上下菜单中选择“确认警报……”。然后输入描述并单击确定
W	黄色	警告	传感器给出错误读数，但 PRTG 会再次尝试。传感器可能很快变为停机状态。此状态的另一个原因可能是传感器的传感器通道设置中设置的警告限制
U	橙子	异常	传感器报告此工作日和时间的异常值。异常检测基于历史平均数据，可以在系统管理中配置或禁用，也可以仅禁用某些组的异常检测避免出现该提示
✓	绿色	正常运行	最后一次扫描没问题，传感器当前正在接收数据
II	蓝色	已暂停	传感器当前暂停（在某个时间段内，无限期地或由依赖性触发）
?	灰色	未知	传感器尚未接收到任何数据，或者（网络）通信中存在错误，可能在探针系统上。如果传感器持续显示此状态，可以尝试重新启动 PRTG

3.3 警报信息处理

PRTG 可以通过 PC 或者 Android/Apple 手机 APP 登录查看设备监控情况，除了日常主动巡查外，PRTG 可以使用通知在发现定义状态（例如传感器速度慢、失败或传感器通道超出阈值）时向网络管理员发送警报，允许使用多个通信渠道中的一个或多个，定义无限数量的通知，通过如电子邮件、SMS、Android 和 iOS 设备推送通知。PRTG 会向用户设置的通知联系人发送通知，而且 PRTG 上的每个用户账户可以单独设置自己的通知。

传感器的状态或数据可以触发通知，可以根据需要

配置外部警报。虽然传感器会激活通知触发器，但是对于组或者设备，可以在层次结构中设置更高的通知触发器，还可以使用继承机制同时为多个传感器设置通知触发器。PRTG 已包含根组的默认通知触发器，如果 PRTG 安装中的任何传感器处于关闭状态达到 10 分钟，则默认通知触发器会触发标准通知电子邮件发送给 PRTG 管理员。

要完成通知设置需要确认以下 4 处设置是否完成：（1）检查并设置通知传递设置，确认 PRTG 将如何以及向哪个收件人发送消息；（2）检查并设置 PRTG 用户的通知联系人，确认接收通知的收件人；（3）检查并设置通知模板，确认通知方法及内容；（4）检查并设置监控目标的通知触发器，确认何时发送通知消息。

结语

PRTG 拥有易用的 Web 界面，丰富的可视化界面，包括实时图表和详细的报表绘制、历史数据变化展示，支持多种协议收集数据，可以收集到网络中几乎所有组件的数据，功能强大且简单易用。PRTG 按照传感器许可购买数量分为多个付费版本，试用期满 30 天的 PRTG，无许可购买，自动恢复为可使用 100 个传感器的永久免费版本。

一个传感器只能监控网络设备的一个方面，例如交换机的一个端口的流量、服务器的 CPU 负载、硬盘的可用空间，分别需要 3 个传感器，平均每台服务器需要大约 15~20 个传感器，每个交换机根据使用情况，可以有选择地监控几个主要的端口信息。对大多数单位而言，没有专职网络管理员，一人多岗，不能做到全天候监控，利用 PRTG 免费版，只对主要的网关、防火墙、交换机及服务器等基础网络设施的关键部位进行安全状态监控，通过合理取舍，100 个传感器完全可以满足日常网络安全管理需求。媒

参考文献

[1] Getting started with PRTG – Academy modules [EB/OL]. https：//www.paessler.com/support/getting-started.

[2] PRTG How-to Guides – Step by step to start with PRTG [EB/OL].https：//www.paessler.com/support/how-to.

[3] PRTG Network Monitor User Manual [EB/OL]. https：//www.paessler.com/manuals/prtg.

（作者单位：新华社北京分社）

（上接第99页）

平台使用率，同时快速促进平台变现，提升经济效益。

结语

知识服务与传统出版相比，具有一定的革新性，但知识服务与传统出版绝不是替代与被替代的关系，而是相辅相成、共同促进的关系。“海关学库”上线后，对中国海关出版社有限公司的品牌提升、纸质图书销售都有明显促进作用，相应的，也有不少用户是购买了纸质图书后寻迹到“海关学库”，再次购买了“通关大神修炼记”等线上课程。这一结果也印证了知识服务与传统出版的相互促进关系。

我们看到，经过几年的探索与实践，大部分出版社在知识服务方面已找到自己的方向、做出一些符合用户需求的产品，有些出版社推出的产品已非常成熟，如人民法院出版社建设的“法信”、人民卫生出版社建设的“人卫智网”，但在职业教育领域，由于互联网教育公司带来的冲击较大，且职业院校的采购方式、采购周期及服务方式等具有较强的特殊性，目前大多出版社在该领域尚未形成规模，可喜的是，随着各出版社不断的探索和实践，道路已越来越清晰。展望未来，专业出版社凭借已有的品牌优势、资源优势、创新精神和转型需求，一定能在职业教育领域打造出适合本社发展的一片新天地。媒

参考文献

[1] 中国数字出版产业年度报告课题组，张立，王飚，李广宇．步入新时代的中国数字出版——2017—2018 中国数字出版产业年度报告（摘要）[J]. 出版发行研究，2018（9）：29-33.

[2] 国务院关于印发国家职业教育改革实施方案的通知 [EB/OL].2019-02-13.http：//www.gov.cn/zhengce/content/2019-02/13/content_5365341.htm.

[3] 孙真福．教育出版数字化转型路在何方 [N]. 中国新闻出版广电报，2018-09-03.

[4] 张新新．知识服务向何处去——新闻出版业五种知识服务模式分析 [J]. 出版与印刷，2019（1）：1-5.

（作者单位：中国海关出版社有限公司）